August 19, 2016

North Dakota State and Local Intelligence Center

Bi-Weekly Cyber Rollup

Included in this week's summary:
Click on the Section Header to go directly to that location in the Summary

NORTH DAKOTA & REGIONAL

(U) Audit identifies 'fundamental weakness' in N.D. network but IT chief says systems secure

(U) Mike Ressler noted the network hasn't experienced a major breach since June 2015, when an unauthorized user gained access to a state server containing incident and payroll reports made to Workforce Safety & Insurance, the state's workers' compensation agency. The server also held data for the Health Department and the Teachers' Fund for Retirement, but ITD said there was no evidence of personally identifiable information being removed.

Source: (U) http://www.grandforksherald.com/news/4091928-audit-identifies-fundamental-weakness-nd-network-it-chief-says-systems-secure

(U) St. Paul police looking for suspects in ATM skimming cases

(U) A man walked up to a St. Paul drive-through ATM on a Monday at 6:06 a.m. with a green device in his hands and a minute later he was done. He'd attached a "skimmer." The next week, a man working with him put a skimmer on another St. Paul ATM. In both cases, the electronic devices allowed tens of thousands of dollars to be stolen from at least 100 people, according to police.

Source: (U) http://www.twincities.com/2016/08/16/st-paul-police-looking-for-suspects-in-atm-skimming-cases/

NATIONAL

(U) NSA's Hacking Group Hacked! Bunch of Private Hacking Tools Leaked Online

(U) An unknown hacker or a group of hackers just claimed to have hacked into "Equation Group" -- a cyber-attack group allegedly associated with the United States intelligence organization NSA -- and dumped a bunch of its hacking tools (malware, private exploits, and hacking tools) online.

Source: (U) http://thehackernews.com/2016/08/nsa-hacking-tools.html

(U) Massive Email Bombs Target.Gov Addresses

(U) Over the weekend, unknown assailants launched a massive cyber attack aimed at flooding targeted dot-gov (.gov) email inboxes with subscription requests to thousands of email lists. According to experts, the attack — designed to render the targeted inboxes useless for a period of time — was successful largely thanks to the staggering number of email newsletters that don't take the basic step of validating new signup requests.

Source: (U) http://krebsonsecurity.com/2016/08/massive-email-bombs-target-gov-addresses/

INTERNATIONAL

(U) Linux botnets dominate the DDoS landscape

(U) Kaspersky Lab released its distributed denial-of-service (DDoS) Intelligence Report which reported that Linux botnets accounted for 70.2 percent of all DDoS attacks initiated during quarter 2 (Q2) of 2016, while only 44.5 percent of DDoS attacks were carried out by Linux botnets in quarter 1. The report also stated that SYN DDoS attacks were the most popular methods for DDoS attacks during Q2, followed by transmission control protocol (TCP), Hypertext Transfer Protocol Secure (HTTP), and Internet control message protocol (ICMP) floods.

Source: (U) http://news.softpedia.com/news/linux-botnets-dominate-the-ddos-landscape507043.shtml

(U) Remote Butler attack; APT groups' dream come true

(U) Microsoft security researchers developed an extension of the "Evil Maid" attack dubbed "Remote Butler" which allows attackers to bypass local Windows authentication to defeat full disk encryption without physical access to the targeted device. A patch released by Microsoft for the "Evil Maid" attack also prevents attackers from carrying out a "Remote Butler" attack.

Source: (U) https://www.helpnetsecurity.com/2016/08/08/remote-butler-attack/

(U) DDoSCoin – New Crypto-Currency Pays Users for Participating in DDoS Attacks

(U) It's 2016, and now, you can earn some dollars by contributing into well-organized DDoS attack scheme. Do you know while mining Bitcoins you are actually contributing a significant computational power to keep the Bitcoin network running? In Bitcoins, the miners actually build and maintain massive public ledger containing a record of every Bitcoin transaction in history.

Source: (U) http://thehackernews.com/2016/08/ddoscoin-cryptocurrency.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Security+Blog%29&_m=3n.009a.1300.iv0ao09bj9.rae

(U) Data of nearly 2 million users exposed in Dota2 forum hack

(U) Researchers from LeakedSource reported that the Dota2 official developers forum was breached after hackers stole the usernames, email addresses, user identifiers, passwords, and IP addresses of nearly 2 million of the forum's users July 10 by hashing and salting the password with the MD5 algorithm. Forum administrators patched the vulnerability and reset all user account passwords.

Source: (U) http://news.softpedia.com/news/data-of-nearly-2-million-users-exposed-indota2-forum-hack-507162.shtml

(U) Linux flaw allows attackers to hijack web connections

(U) Researchers from the University of California at Riverside and the U.S. Army Research Laboratory discovered a vulnerability affecting the Transmission Control Protocol (TCP) specification implemented in Linux kernel could be leveraged to intercept TCP-based connections between two hosts on the Internet, to track users' activity, terminate connections, and inject arbitrary data into a connection after an off path attacker deduced the sequence numbers that identify TCP data packets exchanged between hosts using the Internet Protocol (IP) addresses of the targeted communicating devices. Developers of various Linux distributors were working to fix the security hole.

Source: (U) http://www.securityweek.com/linux-flaw-allows-attackers-hijack-webconnections

(U) Chrome, Firefox, and IE browser hijacker distributed via legitimate software

Intel McAfee security researchers discovered recent versions of the Bing.vc malware were being delivered to Google Chrome, Mozilla Firefox, and Microsoft's Internet Explorer via legitimate-looking applications distributed by Lavians Inc., in order to take over the Website's homepage and insert ads into visited sites, and redirect all users to Bing.vc in an attempt to sell victims an expensive utility to fix the browser hijacking problem. Researchers stated users must remove the registry keys or use an automated PC clean-up utility, as well as clean the shortcuts for each browser in order clear the malware from an infected app.

Source: (U) http://news.softpedia.com/news/chrome-firefox-and-ie-browser-hijackerdistributed-via-legitimate-software-507183.shtml